Data Processing Contract (General Purposes)

Preamble

The NPCC, as a Controller, is under a legal obligation to ensure that when it processes personal data for any purpose **other than** any of the Law Enforcement Purposes it does so in compliance with the UK GDPR and Data Protection Act 2018 (DPA).

Where the NPCC directs another organisation or person to process personal data on its behalf, that organisation or person is known as a Processor.

The NPCC remains responsible for ensuring that any processor also processes personal data in compliance with the DPA. Specifically, the NPCC must ensure that suitable arrangements are in place to protect the security of the personal data in question, as required by UK GDPR Article 28 states:

> *1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*
>
> *2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.*
>
> *3. Processing by a processor shall be governed by a contract or other legal act under domestic law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*
>
> > *(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by domestic law; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*
> >
> > *(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
> >
> > *(c) takes all measures required pursuant to Article 32;*
> >
> > *(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;*
> >
> > *(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*
> >
> > *(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;*
> >
> > *(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless domestic law requires storage of the personal data;*
> >
> > *(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*
>
> *With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or domestic law relating to data protection.*
>
> *4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under domestic law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.*
>
> *5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate*

sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraph 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7…

8. The Commissioner may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

The associated UK GDPR Recital 81 states:

To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

UK GDPR Article 29 states:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Compliance with the UK GDPR Article 28 and UK GDPR Article 29 requirements is best achieved through use of a document known as a Data Protection Contract (DPC) drawn up between the NPCC and any processor working on its behalf.

The NPCC has therefore developed a template for a DPC which commences overleaf. The text highlighted in yellow should be replaced with appropriate content relevant to the processing in question.

Advice on completion of the template can be obtained from the NPCC's Data Protection Officer.

Note: Where the processing is than for any of the Law Enforcement Purposes that activity falls under the DPA Part 3. A separate Data Processing Contract template has been developed for that alternative scenario in recognition of the differing legislation that applies to General Processing and Law Enforcement Purposes processing respectively.

The Contract

This Contract is made on 11 December 2023 between the parties:

The National Police Chiefs' Council (NPCC) (the **Controller**) of 10 Victoria Street, London SW1H 0NN (Information Commissioner Registration Number ZA495495); and

Police Digital Service of 20 Gresham Street, London EC2V 7JE with registered number 08113293 (Information Commissioner Registration Number ZA112970) (the **Processor**).

This Contract sets out the terms and conditions under which the Controller discloses personal data held by it to the Processor, and the Processor uses that personal data in the performance of tasks mandated by the Controller. Any processing of Personal Data by the Processor must comply with the provisions of this Contract.

1. Definitions

The following words and phrases used in this Contract shall have the following meanings except where the context otherwise requires:

Authorised Staff means those individuals set out in Appendix A: Details of Processing and any other individuals expressly authorised in writing by the Controller to process NPCC Data.

Confidential Information means all NPCC Data and any other information relating to the Controller's users and prospective users, current or projected financial or trading situations, operating plans, operating strategies, developments and all other information relating to the Controller's affairs including any trade secrets, know-how, and any information of a confidential nature imparted by the Controller to the Processor during the term of this Contract or coming into existence as a result of the Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

Contract means this Data Processing Contract together with its appendices and all other documents attached to or referred to as forming part of this Contract.

Data Protection Impact Assessment means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data. See UK GDPR Article 35

Data Protection Legislation means: (i) the UK GDPR; (ii) the DPA; and (iii) all applicable laws relating to the Processing of Personal Data and privacy.

Data Subject, **Processing**, **Personal Data**, **Personal Data Breach**, and **Sensitive Processing** have the same meaning as in Article 4 of the UK GDPR.

Data Subject Rights Request means an application made by, or on behalf of, a Data Subject in accordance with rights granted to Data Subjects pursuant to the Data Protection Legislation.

DPA means the Data Protection Act 2018.

UK GDPR is defined at Section 3(10) of the DPA.

Party means a party to this Contract.

NPCC Data means any data, including Personal Data, and data subject to sensitive processing, to be Processed by the Processor on behalf of the Controller under this Contract, as set out in Appendix A.

NPCC Manager means **S40(2)** who has oversight and responsibility for ensuring the processing on behalf of the Controller or other such person as shall be notified to the Processor from time to time complies with the terms of this Contract. The NPCC Manager, with assistance from the NPCC Data Protection Officer and Freedom of Information lead will assume responsibility for co-ordinating data protection compliance, notification, security, confidentiality, audit and co-ordination of Data Subject Rights and Freedom of Information requests, as directed by the terms of this Contract.

Processor Manager means **S40(2)** Head of Data Services who has day-to-day management responsibility for the processing and compliance with this Contract on behalf of the Processor or such other person as shall be notified to the Controller from time to time. The Processor Manager will assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of Data Subject Rights and Freedom of Information requests for the Processor as directed by the terms of this Contract.

Protective Measures means appropriate technical and organisational measures to ensure a level of security of Personal Data appropriate to the risk of processing, in accordance with Data Protection Legislation.

Purpose means the purpose of the processing as set out in Appendix A.

Services means the processing activity and services to be undertaken by the Processor on behalf of the Controller, as identified in Appendix A.

2. Compliance with law, the Purpose and the Controller's instructions

The details of the processing of NPCC Data envisaged by this Contract are set out in Appendix A, and the Processor shall only process NPCC Data in accordance with Appendix A. Where deviation from Appendix A is required, this will only occur where previously authorised in writing by the NPCC Manager to the Processor Manager.

The Processor shall process the NPCC Data:

a) in accordance with the Data Protection Legislation;

b) only for the Purpose; and

c) only on the documented instructions of the Controller, including as set out in Appendix A.

The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

The Processor shall:

d) pay any data protection fees to, and/or register any processing particulars with the Information Commissioner's Office (ICO) as required by the Data Protection Legislation;

e) designate a data protection officer if required by the Data Protection Legislation; and

f) maintain complete and accurate records and information of its processing of NPCC Data.

The Purpose is consistent with the original purpose of the Personal Data creation and/or collection, which assists the Controller in fulfilling their obligations to protect life and property, preserve order, prevent the commission of offences, bring offenders to justice, and any duty or responsibility arising from common or statute law.

Controllership of the NPCC Data shall at all times remain with the Controller.

3. Access to the NPCC Data

Access to the NPCC Data will be restricted to the Authorised Staff. The Processor will take all reasonable steps to ensure the reliability and integrity of the Authorised Staff and will ensure that the Authorised Staff:

a) are aware of and comply with the Processor's duties under this Contract;

b) are subject to appropriate confidentiality obligations with regard to the NPCC Data;

c) are informed of the confidential nature of the NPCC Data and do not publish, disclose or divulge any NPCC Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and

d) have undergone adequate training in the use, care, protection and handling of Personal Data.

4. Security of NPCC Data

The Processor recognises that the Controller has obligations relating to the security of data under their controllership under the Data Protection Legislation, Her Majesty's Government's Information Assurance Standards, and the National Police Chiefs' Council's Community Security Policy. The Processor will continue to apply those relevant obligations as detailed below on behalf of the Controller during the term of this Contract and will assist the Controller in complying with the Controller's security

obligations under the Data Protection Legislation.

The Processor shall ensure that it has in place Protective Measures, which protect NPCC Data against a Personal Data Breach, taking into account:

a) the nature of the NPCC Data;

b) the harm that might result from a Personal Data Breach;

c) the state of technological development; and

d) the cost of implementing measures.

The Protective Measures shall include, as a minimum, those measures set out in **Appendix B: Baseline Security Requirements**. In particular, the Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport;
- deter deliberate compromise or opportunist attack; and
- promote discretion in order to avoid unauthorised access.

During the term of this Contract, the Processor Manager shall carry out any checks as are reasonably necessary to ensure that the above arrangements are not compromised.

The Controller will undertake any suitability checks on any persons having access to police premises and the NPCC Data and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Processor will ensure that each person who will participate in the Purpose understands this and will provide all required assistance to enable the Controller to exercise its rights under this provision.

The Controller reserves the right to undertake a review of security provided by any Processor and may request reasonable access during normal working hours to the Processor's premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will result in the termination of this Contract.

5. Sub-processors

Before allowing any third-party Processor (a **Sub-processor**) to process NPCC Data, the Processor must:

a) notify the Controller in writing of the intended Sub-processor and the processing intended to be carried out by that Sub-processor;

b) obtain the Controller's written consent to the use of that Sub-processor;

c) enter into a written contract with the Sub-processor imposing on the Sub-processor terms that are substantially equivalent to those set out in this Contract in respect of the NPCC Data; and

d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

6. Transfers beyond the UK

The Processor shall not transfer NPCC Data beyond the UK unless the Controller's prior written consent is obtained and the following conditions are fulfilled:

a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer in accordance with Chapter V (Articles 44 to 49) of the UK GDPR and any other applicable Data Protection Legislation, as determined by the Controller;

b) the Data Subject has enforceable rights and effective legal remedies;

c) the Processor complies with its obligations under the Data Protection Legislation in respect of such transfer; and

d) the Processor complies with any reasonable instructions notified to it by the Controller with respect to the transfer.

7. Data Subject Rights Application

The Processor shall:

a) notify the Controller immediately (and in any event within two business days) if it receives a Data Subject Rights Application (or purported Data Subject Rights Request) relating to the NPCC Data;

b) provide the Controller with full details and copies of the Data Subject Rights Application; and

c) provide full assistance to the Controller to enable the Controller to comply with a Data Subject Rights Application within the relevant timescales set out in the Data Protection Legislation.

8. Personal Data Breaches and data protection communications

The Processor shall:

a) notify the Controller immediately (and in any event within 24 hours) upon becoming aware of a Personal Data Breach affecting the NPCC Data, including full details of the Personal Data Breach;

b) notify the Controller immediately (and in any event within two business days) if it receives any claim, request, complaint, notification or communication from a Data Subject, ICO or another third party relating to either Party's processing of the NPCC Data (a **Data Protection Communication**) and provide the Controller will full details and copies of the Data Protection Communication; and

c) provide the Controller will full assistance following any Personal Data Breach or the receipt of any Data Protection Communication to enable the Controller to handle such Personal Data Breach or Data Protection Communication in accordance with the Controller's obligations under Data Protection Legislation.

The Processor shall not contact any Data Subject directly or respond to a Data Subject Rights Application or Data Protection Communication without the Controller's prior written consent or as permitted by Appendix A.

The Processor's obligations to notify the Controller under this clause 8 shall include an obligation to provide further information to the Controller in phases, as details become available, if full information is not available at the time of notification.

9. Data Protection Impact Assessments

The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment relating to the processing of the NPCC Data. Such assistance may, at the discretion of the Controller, include:

a) assisting the Controller in preparing a systematic description of the envisaged processing operations and the Purpose;

b) assisting the Controller in conducting an assessment of: i) the necessity and proportionality of the processing operations in relation to the Purpose; and ii) the risks to the rights and freedoms of Data Subjects; and

c) providing the Controller with full information about the Protective Measures in place.

The Processor shall provide all reasonable assistance to the Controller in complying with the Controller's obligations to carry out prior consultation with the ICO in accordance with the Data Protection Legislation.

10. Retention, Review and Deletion

The NPCC Data will be retained by the Processor and then securely disposed by the Processor when no longer required for the Purpose, in accordance with Appendix A. In any event, on termination of the Contract, the Processor shall, at the written direction of the Controller, delete or return Personal Data

(and any copies of it) to the Controller unless the Processor is required by law to retain the Personal Data.

11. Audit

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations in this Contract and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

Upon request, the Processor shall allow the Controller, the ICO and their representatives access to its premises, records and personnel for the purpose of assessing the Processor's compliance with its obligations under this Contract.

12. Human Rights & Freedom of Information

The processing of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Contract by the Data Protection Legislation and the Human Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the Parties to this Contract.

The Parties agree and declare that the information accessed pursuant to this Contract will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportionate, having regard to the purposes of the Contract and the steps taken in respect of maintaining a high degree of security and confidentiality.

If any Party to this Contract receives a request for information under the provisions of the Freedom of Information Act 2000 identified as originating from another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of that Act.

13. Confidentiality

The Processor shall not divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or with the prior written authority of the Controller) any Confidential Information, which it shall treat as private and confidential and safeguard accordingly. The restriction in this paragraph shall not apply where disclosure of the Confidential Information is ordered by a court of competent jurisdiction or is otherwise required by any law or regulation to which the Processor is subject. In such a case, the Processor shall immediately notify the Controller in writing of any such requirement for disclosure of the Confidential Information in order to allow the Controller to make representations to the person or body making the request.

The Processor shall ensure that any individuals who have access to Confidential Information under this Contract are aware of their responsibilities in connection with the use of that Confidential Information.

For the avoidance of doubt, the obligations of confidentiality imposed on the Parties by this Contract shall continue in full force and effect after the expiry or termination of this Contract.

The restrictions contained within this section 13 of this Contract shall cease to apply to any information which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Contract.

14. Indemnity

In consideration of the provision of the NPCC Data for the Purpose the Processor undertakes to indemnify and keep indemnified the Controller against any liability which may be incurred by the Controller as a result of the Processor's breach of this Contract, provided that this indemnity shall not apply to the extent that the liability arises from information supplied by the Controller which is shown to have been incomplete or incorrect, unless the Controller establishes that the error did not result from any wilful wrongdoing or negligence on their part.

15. Disputes

In the event of any dispute or difference arising between the Parties out of this Contract, the NPCC Manager and the Processor Manager shall meet in an effort to resolve the dispute or difference in good faith.

The Parties will, with the help of the Centre for Effective Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

16. Term and Termination

This Contract will terminate on the completion date of project or whenever the Purpose is completed, whichever is the sooner.

The Controller may at any time by notice in writing terminate this Contract forthwith if the Processor is in material breach of any obligation under this Contract.

At the discretion of the Controller, this Contract may be terminated by the Controller after the replacement of the Processor Manager.

Either Party may terminate this Contract by giving 30 days' notice in writing to the other Party.

Notwithstanding termination of this Contract, clauses 2 to 15 of this Contract shall survive termination to the extent that the Processor continues to Process NPCC Data on behalf of the Controller.

17. Variation

The Controller will have the final decision on any proposed variation to this Contract. No variation of the Contract shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Contract, save that:

a) the Controller may, at any time on not less than 30 business days' notice, revise this Contract by replacing all or part of it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract); and

b) the Parties agree to take account of any guidance issued by the ICO and the Controller may, on not less than 30 business days' notice, amend this Contract to ensure that it complies with any guidance issued by the ICO.

18. Miscellaneous

This Contract acts in fulfilment of part of the responsibilities of the Controller as required by Article of 28 the UK GDPR.

This Contract constitutes the entire agreement between the Parties as regards its subject matter and supersedes all prior oral or written agreements regarding such subject matter.

If any provision of this Contract is held by a court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Contract, which shall remain in full force and effect.

The validity, construction and interpretation of the Contract and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract and, unless otherwise stated, references to clauses and appendices are references to the clauses of and appendices to this Contract.

Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any

subordinate legislation made under it.

The word ‘including’ shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word ‘include’ and its derivatives shall be construed accordingly.

On behalf of the NPCC:

Signed: **S40(2)**

Print: Chief Constable Charlie Hall

Date 27 November 2023

On behalf of Police Digital Service

Signed: **S40(2)**

Print: Ian Bell

Date: 11th December 2023

Appendix A: Details of Processing

The Processor shall comply with any further written instructions with respect to processing from the Controller. Any such further instructions shall be incorporated into this Appendix.

Subject matter of the Processing	**S31(1)** on the new PDS Platform with proven operational success. The intention is now to continue to host the tool on the PDS Platform for a further timebound period, with a view to being made available nationally in future if the trial is successful.
Duration of the Processing	The processing under this agreement is for a further period of up to 6 months, beginning 28th June 2024. Should further national expansion be conducted, a further DPC would be sought for production.
Purpose of the Processing	**S31(1)** The purpose is not incompatible with the original law enforcement purpose for which the personal data was collected: namely two of the law enforcement purposes: • The prevention, investigation, detection or prosecution of criminal offences, and • The prosecution of criminal offences or the execution of criminal offences, in relation to the unlawful supply of drugs.
Nature of the Processing	• Processing will be in line with the National ANPR Standards for Policing and Law Enforcement (NASPLE) https://www.gov.uk/government/publications/national-anpr-standards • **S31(1)** **S31(1)** **S31(1)** This DPC references: 1. The updated DPIA for this tool. 20240515- DPIA Find and Profile C3147 County Lines - Extension.docx

	2. The NAS DPIA: https://assets.publishing.service.gov.uk/media/6295d105d3bf7f036ddfe7bd/ANPR__DPIA_V3.0_approved.pdf 3. The National ANPR Standards for Policing and Law Enforcement (NASPLE)
Type of Personal Data	**NAS ANPR data** ANPR data is the capture of a Vehicle Registration Mark and other data as a vehicle passes an ANPR camera. The full details of the NAS dataset are available in the Home Office National ANPR Service Technical Specifications but for the purpose of this project it is expected only the following fields will be required: • VRM – the registration number of the vehicle • Time of the capture • Location of the camera. • Make, model and colour of vehicle **S31(1)**
Categories of Data Subject	Offenders, Suspects, Victims, Police Officers, Members of the public.
Arrangements for return or destruction of the data once processing is complete	Data uploaded to the Find and Profile Tool will be retained on PDS systems only for up to 24hrs, as an automated daily deletion process is in place at 0300hrs. No PDS individuals will have to review this data. Data of continued relevance to ROCU investigations may also be retained locally by them under provisions of the Criminal Procedure and Investigations Act (CPIA) or the Management of Police Information (MOPI) principles as appropriate.
Authorised Staff	**S31(1)**

Appendix B: Baseline Security Requirements for Data Processing Contracts

Requirements

The Processor will put in place appropriate physical, technical and organisational measures to protect any information provided to them under this Contract.

The Processor must ensure that any of their personnel are able to access only the NPCC Data necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to personal data and Data Protection Legislation.

The Processor will maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.

The Processor will protect the physical security of the NPCC Data. This means they will, as a minimum:

- Ensure their organisation controls physical access to its premises;
- Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises;
- Ensure proper physical control of printers and photocopiers so that personal information is not left lying on printers/photocopiers;
- Ensure secure disposal of printed materials, so that materials intended for disposal do not remain accessible. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises;
- Ensure that old computers, printers, and other electronic equipment are disposed of safely and that all personal information is irretrievably deleted from any memory before disposal.

The Processor will protect the electronic security of the NPCC Data. This means they will, as a minimum:

- Ensure their organisation has a strong password policy that is adhered to by all personnel. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members;
- Ensure their organisation installs security patches on electronic devices (including ensuring all operating systems' updates are installed in line with best practice);
- Ensure personnel are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work;
- Ensure that any Wi-Fi connections are secure and that any guest Wi-Fi is on a segregated system, so that guests cannot access other systems from that Wi-Fi;
- Ensure that any information that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice;
- Ensure that their organisation complies with the best practice of cyber security as detailed by the National Cyber Security Centre.

The Processor will ensure that all shared information held on portable devices, including laptops, tablets and USB/portable drives, has full disk encryption. This must be to industry standard, and as a minimum:

- FIPS 140-2/256 bit asymmetrical encryption; or
- CBC-AES 256-bit encryption. A recognised mark of excellence in encryption is CCTM government accreditation (for more information, see the National Cyber Security Centre website).

The Processor will e-mail special category personal data and information about individuals' criminal convictions or offences, suspected or otherwise, only via secure e-mail.

The partners agree to have contracts and systems in place to ensure that any contractors and subcontractors managing any aspect of information security (where approved by the Controller) are fully

aware of and abide by this Contract.

The Processor will have robust data breach reporting policies in place, and adhere to them, so that all personal data breaches are reported immediately to staff responsible for managing data breaches when such breaches become apparent. Further, the Processor must accept that:

- A “personal data breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information which we have transmitted or stored or processed.
- If the personal data breach occurred in the course of information being shared under this ISA, then the organisation/public body who discovers the breach must immediately inform the other partners involved in the sharing of the personal data, particularly the partner who originally shared the information.
- The partners involved will decide who will take the lead on addressing the breach and on whether the breach needs to be reported to the Information Commissioner or to the individuals concerned without undue delay and usually within 72 hours of having become aware of the breach.
- Personal data breaches should trigger an exceptional review of this Contract.